

**Pandora's Hope**

# User Manual



**Version 2**

# |Contents

## **Chapter 1: Router Specifications**

- 1.1 Family Version
- 1.2 Professional Version

## **Chapter 2: Connecting to Pandora's Hope**

- 2.1 Connecting via Wireless Network
  - 2.1a: Windows & Macintosh
  - 2.2b: Mobile Devices
  - 2.2b: Mobile Devices Continued
- 2.2 Connecting via Ethernet
- 2.3 Accessing the Administrative Site

## **Chapter 3: Monitoring Pandora's Hope**

- 3.1 Filter Status
- 3.2 Sites Visited
- 3.3 Sites Blocked
- 3.4 Router Interfaces
- 3.5 DHCP Clients
- 3.6 Diagnostic Tools

## **Chapter 4: The Filtering Mechanism**

- 4.1 Understanding the filter
- 4.2 Configuring the filter
  - 4.2a: The Blacklist
  - 4.2b: The Whitelist
  - 4.2c: The Greylist
  - 4.2d: The Keyword list
  - 4.2e: Filter Level (strength)
  - 4.2f: Search Engine Settings
  - 4.2g: Filtering Categories
  - 4.2h: Excluding Devices
  - 4.2i: Time Restrictions
  - 4.2i: Time Restrictions Continued
  - 4.2j: AdDriven Websites

# |Contents

## Chapter 4: The Filtering Mechanism

4.2k: The Blocking Page

## Chapter 5: System Settings

5.1	Wireless Configuration Settings
	5.1a: Wireless Configuration Settings – Continued
5.2	Network Settings
	5.2a: General Settings: Internet & Local Network
	5.2b: Port Forwarding
	5.2c: DHCP Settings
	5.2d: UPnP Settings
5.3	User Information
5.4	Resetting the Administrative Password

# Chapter 1:

## The Family Version

### 1.1: The Family Version

**Manufacturer:** Buffalo Inc.

**Model Number:** WZR-HP-G300NH2 / WZR-300HP

**Processor Speed:** 400Mhz

**Memory:** 64MB

**Wireless LAN Interface:**

- Standards:** IEEE 802.11n, IEEE 802.11g, IEEE 802.11b

- Access Mode:** Infrastructure

- Antenna:** 2 x 2

- Wireless Security:** WPA2, WEP

**Wired LAN Interface:**

- Speed:** 10/100/1000 Mb/s

- Number of LAN ports:** 4

- Number of WAN ports:** 1

**Dimensions:** 6.2 x 6.5 x 1.4 in

**Weight:** .54 lb

**Power Supply:** External AC 100 – 240V, 50/60 HZ

# Chapter 1:

## Router Specifications

### 1.2: The Pro Version

**Manufacturer:** Buffalo Inc.

**Model Number:** WZR-HP-AG300H / WZR-600DHP

**Processor Speed:** 680Mhz

**Memory:** 128MB

**Wireless LAN Interface:**

- Standards:** IEEE 802.11n, IEEE 802.11g, IEEE 802.11b

- Frequency Range:** 2.4Ghz / 5Ghz

- Access Mode:** Infrastructure

- Antenna:** 2 x 2

- Wireless Security:** WPA2, WEP

**Wired LAN Interface:**

- Speed:** 10/100/1000 Mb/s

- Number of LAN ports:** 4

- Number of WAN ports:** 1

**Dimensions:** 6.2 x 6.5 x 1.4 in

**Weight:** .73 lb

**Power Supply:** External AC 100 – 240V, 50/60 HZ

# Chapter 2:

## Connecting to Pandora's Hope

### 2.1a: Connecting via Wireless Network – Windows & Macintosh

#### -On a Windows PC (XP,Vista,7)

- Select the Wireless Network icon on the task bar



- In that list of networks will be PandorasHope



- Right-click on the PandorasHope network and click connect.
- If prompted for a password, please enter the wireless security key created during the setup wizard.  
**By default it is set to your ten digit telephone number.**

#### -On Mac OSX

- Select the AirPort icon at the top




- Click on the PandorasHope network
- If prompted for a password, please enter the wireless security key created during the setup wizard.  
**By default it is set to your ten digit telephone number.**

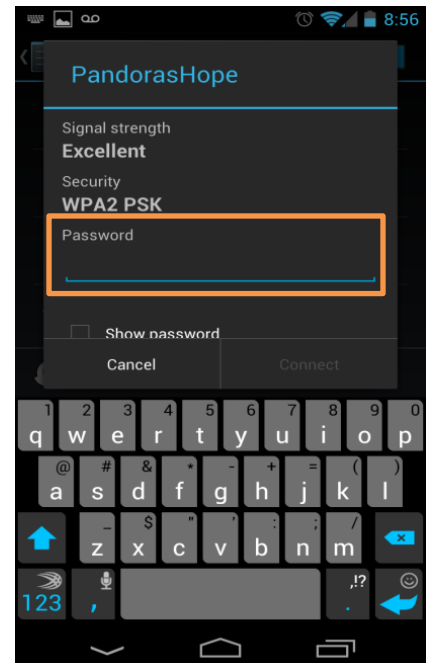
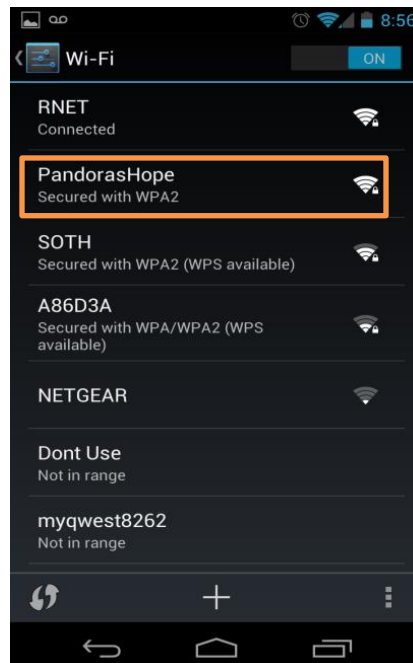
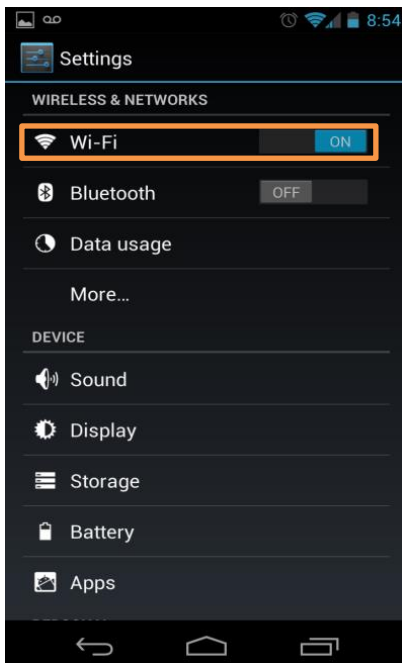
# Chapter 2:

## Connecting to Pandora's Hope

### 2.1b: Connecting via Wireless Network – Mobile Devices

#### -On Android devices

- Select the Settings icon 
- Then select the “Wireless & Networks” menu
- Select “Wi-Fi”, and click on the PandorasHope network
- If prompted for a password, please enter the wireless security key created during the setup wizard.  
**By default it is set to your ten digit telephone number.**




# Chapter 2:

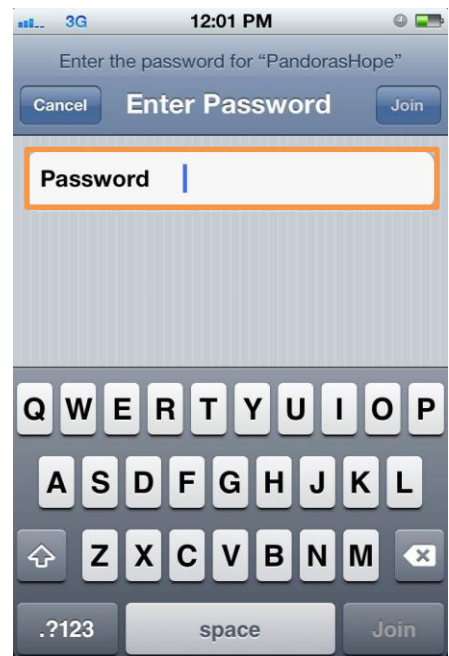
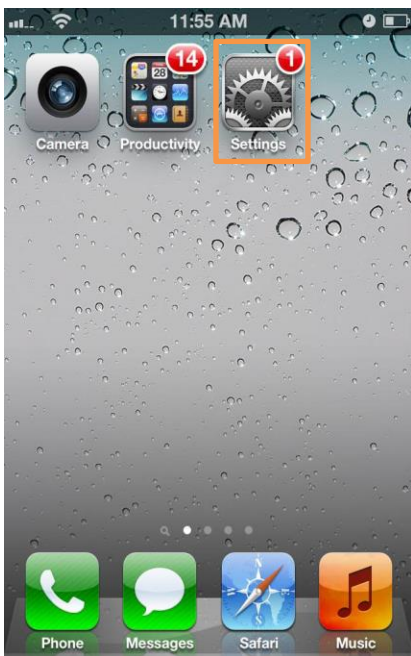
## Connecting to Pandora's Hope

### 2.1c: Connecting via Wireless Network – Mobile Devices (Continued)

-On IOS devices (iPhone, iPod, iPad)

- Select the Settings icon 
- Select "Wi-Fi", and click on the PandorasHope network
- If prompted for a password, please enter the wireless security key created during the setup wizard.

**By default it is set to your ten digit telephone number.**





# Chapter 2:

## Connecting to Pandora's Hope

### 2.2: Connecting via Ethernet

- To connect a device with an Ethernet cable, plug in one end of the ethernet cable into any of the four black ports on the back of the router. Connect the other end into the device.



# Chapter 2:

## The Management Interface

### 2.3: Accessing the Management Interface

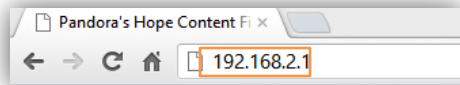
The management interface is an administrative website where the user can access important system settings and filtering tools.

To access the administrative site:

- Open an internet browser, and enter in one of these two addresses into the address bar:

**192.168.2.1**

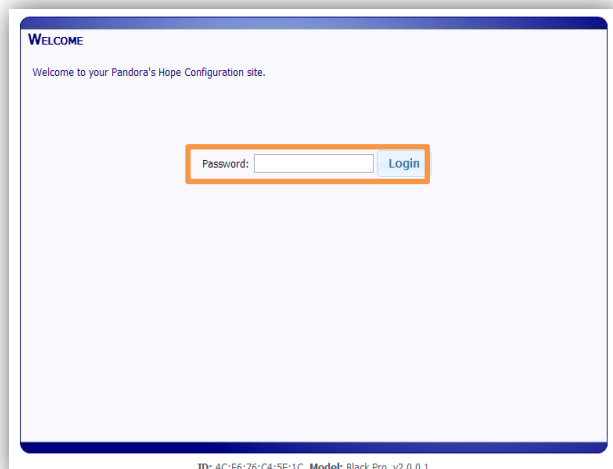
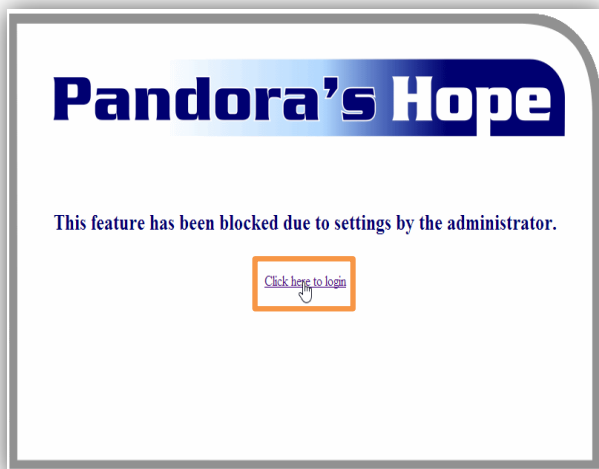
**Local.pandorashope.com**



**Alternatively**, the user could navigate to **Pandorashope.com**, and then select the **My Settings** link at the top of the page.



- The user will then be directed to these pages. Click on the link to login, and enter the administrative password.



# Chapter 3:

## Monitoring Pandora's Hope

### 3.1: Filter Status

**Location:** View Tab > Filter Status

The filter status page displays whether the filter is enabled or disabled. It also will display any temporary bypasses that have been authorized. Please see page [4.3](#) for more information on temporary bypasses.



# Chapter 3:

## Monitoring Pandora's Hope

### 3.2: The Sites Visited Page

**Location:** View Tab > Sites Visited

The sites visited page displays all of the web traffic generated by computers and other devices. This page will provide the device's IP address, the website information, and the exact time that the page was accessed. Pandora's Hope will also archive these logs for later viewing. To select a different date, click on the drop-down menu at the top left-hand corner of the page.

ViewProtectionSystemLogout

Sites Visited

This screen displays the sites that were requested that didn't get blocked by Pandora's Hope.

12/12/2012

Site	Computer	Url	Time
Site: http://news.yahoo.com (19 items)			
http://news.yahoo.com	192.168.2.173	http://news.yahoo.com/_xhr/liveblog/?_...	2012-12-1
http://news.yahoo.com	192.168.2.173	http://news.yahoo.com/_xhr/liveblog/?_...	2012-12-1
http://news.yahoo.com	192.168.2.173	http://news.yahoo.com/_xhr/liveblog/?_...	2012-12-1
http://news.yahoo.com	192.168.2.173	http://news.yahoo.com/_xhr/liveblog/?_...	2012-12-1
http://news.yahoo.com	192.168.2.173	http://news.yahoo.com/_xhr/liveblog/?_...	2012-12-1
http://news.yahoo.com	192.168.2.173	http://news.yahoo.com/_xhr/liveblog/?_...	2012-12-1
http://news.yahoo.com	192.168.2.173	http://news.yahoo.com/_xhr/liveblog/?_...	2012-12-1
http://news.yahoo.com	192.168.2.173	http://news.yahoo.com/_xhr/liveblog/?_...	2012-12-1
http://news.yahoo.com	192.168.2.173	http://news.yahoo.com/_xhr/liveblog/?_...	2012-12-1
http://news.yahoo.com	192.168.2.173	http://news.yahoo.com/_xhr/liveblog/?_...	2012-12-1
http://news.yahoo.com	192.168.2.173	http://news.yahoo.com/_xhr/liveblog/?_...	2012-12-1

ID: 4C:E6:76:C4:5F:1C, Model: Black Pro, v2.0.0.1

# Chapter 3:

## Monitoring Pandora's Hope

### 3.3: The Sites Blocked Page

**Location:** View Tab > Sites Blocked

The sites blocked page will display all of the web traffic that was blocked by Pandora's Hope. This page will provide the device's IP address, the website information, and exact time that the page was blocked. Pandora's Hope will also archive these logs for later viewing. To select a different date, click on the drop-down menu at the top left-hand corner of the page.

The screenshot shows a web interface with a blue header bar containing tabs: View, Protection, System, and a Logout link. Below the header, the main content area is titled "Sites Blocked" and includes a descriptive sentence: "This screen displays the sites and web pages that were requested that got blocked by Pandora's Hope." A date selector dropdown is set to "12/12/2012". Below this is a table with four columns: Site, Computer, Url, and Time. The table lists blocked access to www.ebay.com, www.youtube.com, and local.yahoo.com from IP address 192.168.2.173 on 2012-12-1. The table is scrollable, and a scrollbar is visible on the right side. At the bottom of the page, there is a footer with the text: "ID: 4C:E6:76:C4:5F:1C, Model: Black Pro, v2.0.0.1".

Site	Computer	Url	Time
Site: http://www.ebay.com (6 items)			
http://www.ebay.com	192.168.2.173	http://www.ebay.com/	2012-12-1
http://www.ebay.com	192.168.2.173	http://www.ebay.com/	2012-12-1
http://www.ebay.com	192.168.2.173	http://www.ebay.com/	2012-12-1
http://www.ebay.com	192.168.2.173	http://www.ebay.com/	2012-12-1
http://www.ebay.com	192.168.2.173	http://www.ebay.com/ctg/Apple-iPad-3rd...	2012-12-1
http://www.ebay.com	192.168.2.173	http://www.ebay.com/itm/Girls-Lands-End...	2012-12-1
Site: http://www.youtube.com (1 items)			
http://www.youtube.com	192.168.2.173	http://www.youtube.com/results?search_...	2012-12-1
Site: http://local.yahoo.com (3 items)			
http://local.yahoo.com	192.168.2.173	http://local.yahoo.com/info-63950896-e...	2012-12-1
http://local.yahoo.com	192.168.2.173	http://local.yahoo.com/info-63950896-e...	2012-12-1

ID: 4C:E6:76:C4:5F:1C, Model: Black Pro, v2.0.0.1

# Chapter 3:

## Monitoring Pandora's Hope

### 3.4: The Router Interfaces page

Location: View Tab > Interfaces

The Router Interfaces page displays interface information

The screenshot shows a web interface with a blue header bar containing tabs: View, Protection, System, and a Logout link. The main content area is titled 'Interfaces' and includes a descriptive sentence: 'This screen displays the current status of the interfaces.' Below this, there is a scrollable list of interface details for four interfaces: br-lan, eth0, eth1, and lo. Each interface entry provides a link encapsulation, hardware address, IP address, broadcast address, mask, MTU, metric, and statistics for RX and TX packets, errors, dropped frames, overruns, collisions, and bytes. The interface 'lo' is a local loopback interface with IP 127.0.0.1. At the bottom of the page, the device ID and model are displayed: 'ID: 4C:E6:76:C4:5F:1C, Model: Black Pro, v2.0.0.1'.

Interface	Link encap	HWaddr	inet addr	Bcast	Mask	MTU	Metric	RX packets	RX errors	RX dropped	RX overruns	RX frame	TX packets	TX errors	TX dropped	TX overruns	TX carrier	collisions	txqueuelen	RX bytes	TX bytes
br-lan	Ethernet	4C:E6:76:C4:5F:1C	192.168.2.1	192.168.2.255	255.255.255.0	1500	1	10274	0	0	0	0	15039	0	0	0	0	0	0	1426485 (1.3 MiB)	15248640 (14.5 MiB)
eth0	Ethernet	4C:E6:76:C4:5F:1C				1500	1	9769	0	0	0	0	15533	0	0	0	0	0	1000	1414709 (1.3 MiB)	15399057 (14.6 MiB)
eth1	Ethernet	4C:E6:76:C4:5F:1E	192.168.0.12	192.168.0.255	255.255.255.0	1500	1	18000	0	0	0	0	9061	0	0	0	0	0	1000	15096236 (14.3 MiB)	1146636 (1.0 MiB)
lo	Local Loopback		127.0.0.1		255.0.0.0	16436	1	64	0	0	0	0	64	0	0	0	0	0	0	5472 (5.3 KiB)	5472 (5.3 KiB)

ID: 4C:E6:76:C4:5F:1C, Model: Black Pro, v2.0.0.1

# Chapter 3:

## Monitoring Pandora's Hope

### 3.4: The DHCP Clients page

**Location:** View Tab > DHCP Clients

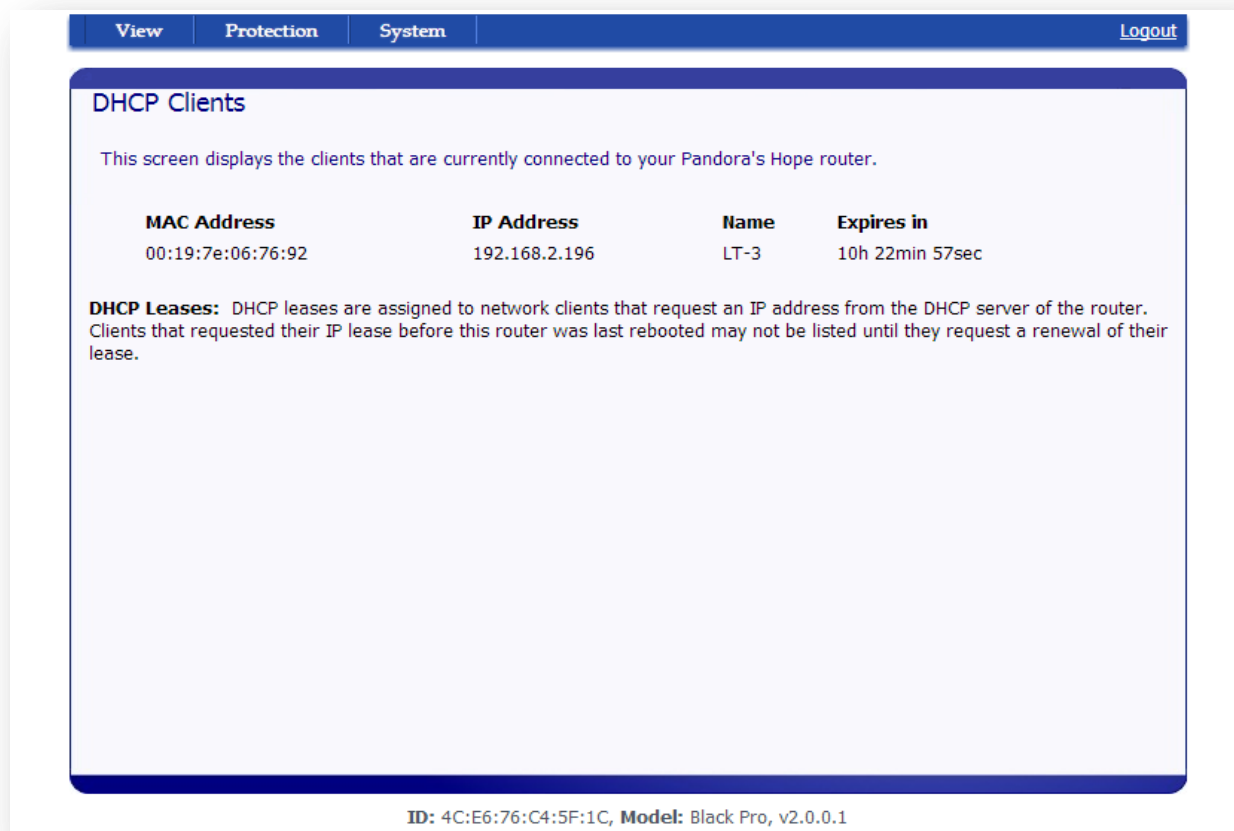
The DHCP Clients page will list all of the devices currently connected to Pandora's Hope. If a device requested its DHCP lease before Pandora's Hope was last rebooted, it will not show in this list until it requests a new lease.

Below are explanations for the various columns:

**MAC Address:** Media Access Control – This address serves as a unique identifier for networked devices.

**IP Address:** Internet Protocol Address – This is an address given to a device by the router.

**Name:** The name field displays the name of the device, either assigned by the user, or manufacturer of the device.



The screenshot shows the 'View' tab selected in the router's interface. The 'DHCP Clients' section is active, displaying a table of connected devices. The table has four columns: MAC Address, IP Address, Name, and Expires in. A single device is listed with MAC Address 00:19:7e:06:76:92, IP Address 192.168.2.196, Name LT-3, and Expires in 10h 22min 57sec. Below the table, a note explains that DHCP leases are assigned to network clients and that clients that requested their IP lease before the router was last rebooted may not be listed until they request a renewal. The footer of the page shows the router's ID as 4C:E6:76:C4:5F:1C and the model as Black Pro, v2.0.0.1.

MAC Address	IP Address	Name	Expires in
00:19:7e:06:76:92	192.168.2.196	LT-3	10h 22min 57sec

**DHCP Leases:** DHCP leases are assigned to network clients that request an IP address from the DHCP server of the router. Clients that requested their IP lease before this router was last rebooted may not be listed until they request a renewal of their lease.

ID: 4C:E6:76:C4:5F:1C, Model: Black Pro, v2.0.0.1

# Chapter 3:

## Monitoring Pandora's Hope

### 3.5: The Diagnostic page

**Location:** View Tab > Diagnostic

**Ping:** This tool will attempt communicate with a specific web or IP address, and will log every “reply” received

**Traceroute:** This tool will attempt to communicate with a specific web or IP address, and will log every “hop” it makes along the way. To use the tool, click on the Traceroute line and enter in an address. The results will populate at the bottom of the page.

**View Log:** This tool will display the entire system log. This includes the output from the start-up phase, and router updates.

**Trigger Remote:** This option allows a user to initiate a remote connection to the Pandora's Hope technical support team. To use Trigger Remote, press the “Trigger Remote” button. If successful, you will receive a confirmation at the bottom of the page.





# Chapter 4:

## The Filtering Mechanism

### 4.1: Understanding the filter

The router works on text-based algorithms to detect inappropriate pages. Each webpage and its URL are dynamically registered against known keywords and phrases that can trigger the blocking mechanism. The filtering system will also check the name, and URL associated with videos and images.

#### **For Text-Based Content**

The filtering system for text-based content will evaluate all of the text on a web page, and register those words against a list of keywords and phrases. The number of keywords permitted on a webpage depends on the filter strength, and the word itself. Some keywords have a greater "weight", and less of them are permitted on a webpage.

#### **For Image-Based Content**

Images are filtered based on their title and URL, evaluated against our list of keywords.

#### **For Video-Based Content**

Videos are filtered based on their title and URL, evaluated against our list of keywords

#### **Ad-blocking**

The filtering system will block advertisements, based on a list on known advertisers.

# Chapter 4:

## The Filtering Mechanism

### 4.2a: Configuring the filter: The Black list

**Location: Protection Tab > Black list**

The black list is a list of websites to be blocked regardless of the content contained on them. This tool is useful for blocking websites that may not be caught by the Pandora's Hope filter, but would still be offensive to the user.

To add an entry into the black list:

- Enter in the web address into the blue area .  
(**Note:** You do not need the prefixes HTTP or WWW.)
- Click the "Add" button
- Once all of the desired addresses have been added, click "Save"
- The newly black listed websites will be blocked immediately after pressing "Save"

To remove an entry from the black list:

- Press the red "X" next to the web address
- Once all of the desired web addresses have been removed, click "Save"

The screenshot shows a web interface for managing a Black List. At the top, there is a navigation bar with tabs for 'View', 'Protection', and 'System', and a 'Logout' link on the right. The main heading is 'Black List'. Below this, a descriptive text states: 'The black list is the list of sites you would like blocked regardless of the content.' There is a section titled 'Add a Site to Black List' which contains a text input field and an 'Add' button. Below the input field, there is a list of three websites already added to the black list, each preceded by a red 'X' icon: 'BadWebSite.com', 'QuestionableContent.org', and 'Netnanny.com'. At the bottom right of the main content area, there are two buttons: 'Reset' and 'Save'. At the very bottom of the page, there is a footer with the text: 'ID: 4C:E6:76:C4:5F:1C, Model: Black Pro, v2.0.0.1'.

# Chapter 4:

## The Filtering Mechanism

### 4.2b: Configuring the filter: The White list

**Location: Protection Tab > White list**

The white list is a list of websites to be permitted regardless of the content contained on them. This tool is useful for allowing websites that may be incorrectly targeted by the Pandora's Hope filter. To add an entry into the white list:

- Enter in the web address into the blue area .  
(Note: You do not need the prefixes HTTP or WWW.)
  - Click the "Add" button
  - Once all of the desired addresses have been added, click "Save"
  - The newly white listed websites will be permitted immediately after pressing "Save"
- Important! Any web address in the white list will be UNFILTERED.**

To remove an entry from the Whitelist:

- Press the red "X" next to the web address
- Once all of the desired web addresses have been removed, click "Save"

The screenshot shows a web interface for configuring a 'White List'. At the top, there are tabs for 'View', 'Protection', and 'System', with 'Protection' being the active tab. A 'Logout' link is in the top right corner. The main heading is 'White List'. Below it, a paragraph explains: 'The white list is the list of sites you would like allowed regardless of the content. Only include sites that you know to be clean such as church, medical, or addition recovery but that might be inaccurately blocked.' There is a section titled 'Add a Site to White List' which contains a text input field and an 'Add' button. Below this, a list of websites is shown, each preceded by a red 'X' icon, indicating they are currently blocked or in the process of being added/removed. The websites listed are: lds.org, nflximg.com, llnwd.net, movies.netflix.com, xbox-ecn102.vo.msecnd.net, download.xbox.com, download.xbox.com.edgesuite.net, imagery.wxc.com, and envelopesexpress.com. At the bottom right of the list, there are 'Reset' and 'Save' buttons. At the very bottom of the page, a footer displays the ID: 4C:E6:76:C4:5F:1C and Model: Black Pro, v2.0.0.1.

View Protection System Logout

### White List

The white list is the list of sites you would like allowed regardless of the content. Only include sites that you know to be clean such as church, medical, or addition recovery but that might be inaccurately blocked.

#### Add a Site to White List

Add

- X lds.org
- X nflximg.com
- X llnwd.net
- X movies.netflix.com
- X xbox-ecn102.vo.msecnd.net
- X download.xbox.com
- X download.xbox.com.edgesuite.net
- X imagery.wxc.com
- X envelopesexpress.com

Reset Save

ID: 4C:E6:76:C4:5F:1C, Model: Black Pro, v2.0.0.1

# Chapter 4:

## The Filtering Mechanism

### 4.2c: Configuring the filter: The Grey List

**Location: Protection Tab > Grey list**

The Grey list is a list of websites to be permitted regardless of their URL. This tool is useful for allowing websites whose addresses may targeted by the Pandora's Hope filter.

**To add an entry into the Grey list:**

- Enter in the web address into the blue area .  
(**Note:** You do not need the prefixes HTTP: or WWW.)
- Click the "Add" button
- Once all of the desired addresses have been added, click "Save"
- The newly grey listed websites will be permitted immediately after pressing "Save"

**To remove an entry from the grey list:**

- Press the red "X" next to the web address
- Once all of the desired web addresses have been removed, click "Save"



# Chapter 4:

## The Filtering Mechanism

### 4.2d: Configuring the filter: The Keyword List

**Location: Protection Tab > Keyword list**

The Keyword List is a user defined list of keywords and phrases to be used by the filtering system to block content. Websites containing these keywords and phrases will be blocked, regardless of any other content contained on them. This tool is useful for customizing the type of content Pandora's Hope will block.

**To add an entry into the Keyword List:**

- Enter in the words or phrases into the area labeled: "Add Keyword or Phrase"
- Hit the enter key when the word or phrase has been typed out.
- The newly added keyword or phrase will then be displayed in a white box.
- Once all of the desired keywords or phrases have been entered, click the "Save" button

**To remove an entry from the keyword list:**

- Press the blue "X" next the word or phrase
- Once all of the desired keywords or phrases have been removed, click "Save"

The screenshot shows a web interface with a blue header bar containing tabs: 'View', 'Protection', 'System', and a 'Logout' link. The 'Protection' tab is active. Below the header is a section titled 'Key Word List'. Inside this section, there is a text area with the following instructions: 'This is a list of key words and phrases that should trigger a block. If sites contain the specified words or phrases they will be blocked. Use alphabetic characters, +, -, underline, spaces and exclamation, question signs. To finish an input use comma or enter'. Below the text area is a text input field with the placeholder text 'Example X Add Key Word or Phrase'. At the bottom right of the 'Key Word List' section are two buttons: 'Reset' and 'Save'. At the very bottom of the page, there is a small text string: 'ID: 4C:E6:76:C4:5F:1C, Model: Black Pro, v2.0.0.1'.

# Chapter 4:

## The Filtering Mechanism

### 4.2e: Configuring the filter: The Filter Level

**Location: Protection Tab > Filter Level**

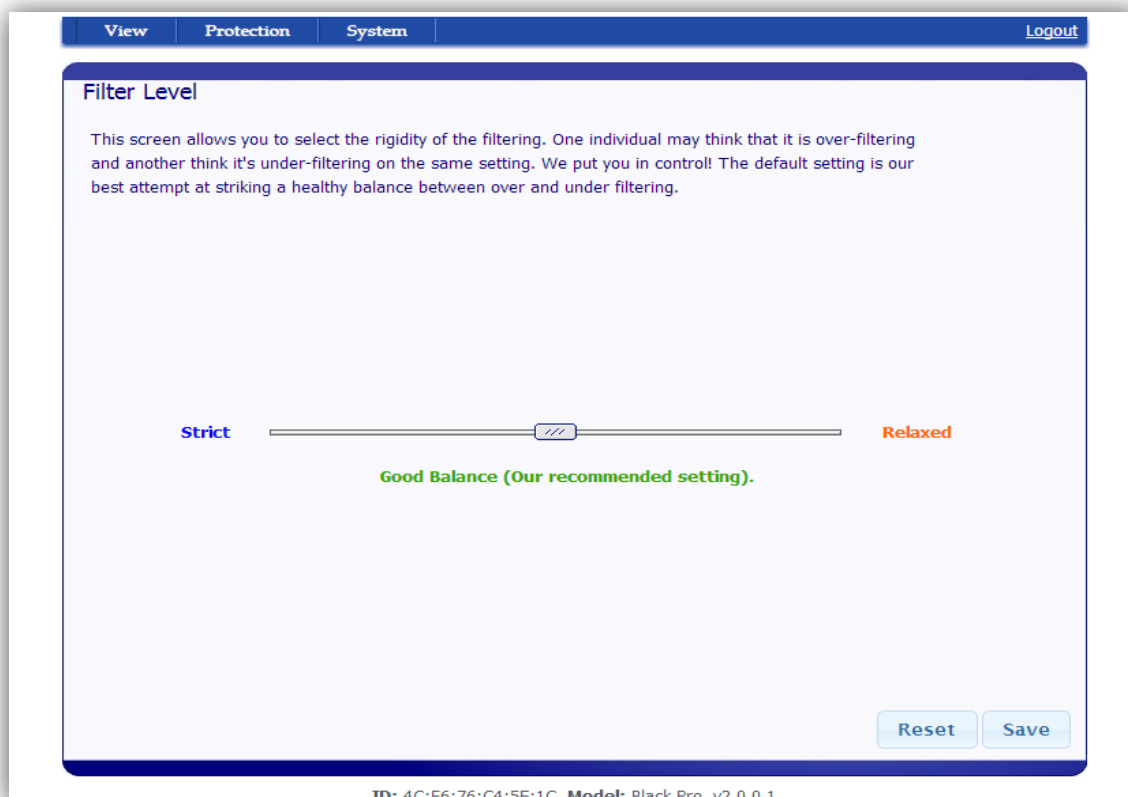
The Filter Level tool allows a user to easily adjust the rigidity of the filter. By default, the filter is set to “Good Balance”.

**To increase the filter strength:**

- Move the slider to the left in small increments, repeating as necessary. As the slider moves more to the left, the user will receive indicator messages.
- Click “Save” once the filter level has been set

**To decrease the filter strength:**

- Move the slider to the right in small increments, repeating as necessary. As the slider moves more to the right, the user will receive indicator messages.
- Click “Save” once the filter level has been set



# Chapter 4:

## The Filtering Mechanism

### 4.2f: Configuring the filter: Search Engine Settings

**Location:** Protection Tab > Search Engine Settings

The Search Engine Settings page allows the user to customize certain functions related to Google Search.

➤ **Allow Google Images:**

This feature will enable or disable the use of Google Images. By default it is set to off.

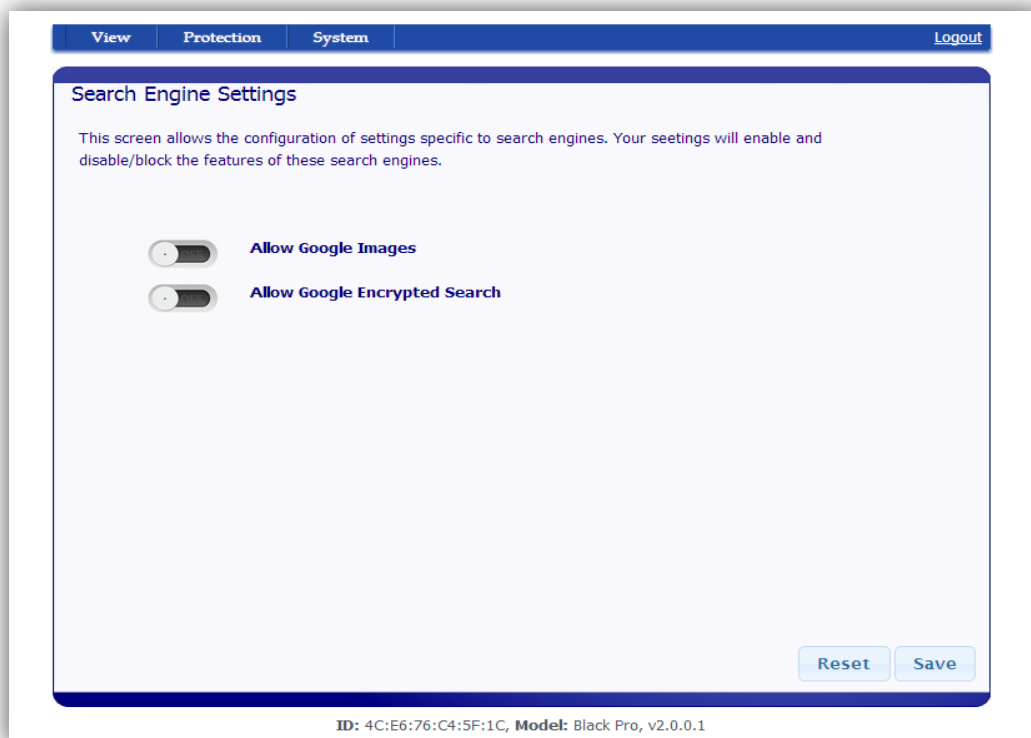
To allow the use of Google Images, click on the corresponding button. The switch will turn yellow to indicate that it has been activated. Click the “Save” button once all desired options have been activated.

**Important: Google Images can present a serious internet safety risk, and is best blocked, or used with discretion.**

➤ **Allow Google Encrypted Search:**

This feature will allow the user to permit the use of encrypted Google searches through: <https://Google.com>

**Important: Encrypted searches cannot be filtered, and may return undesired results.**



# Chapter 4:

## The Filtering Mechanism

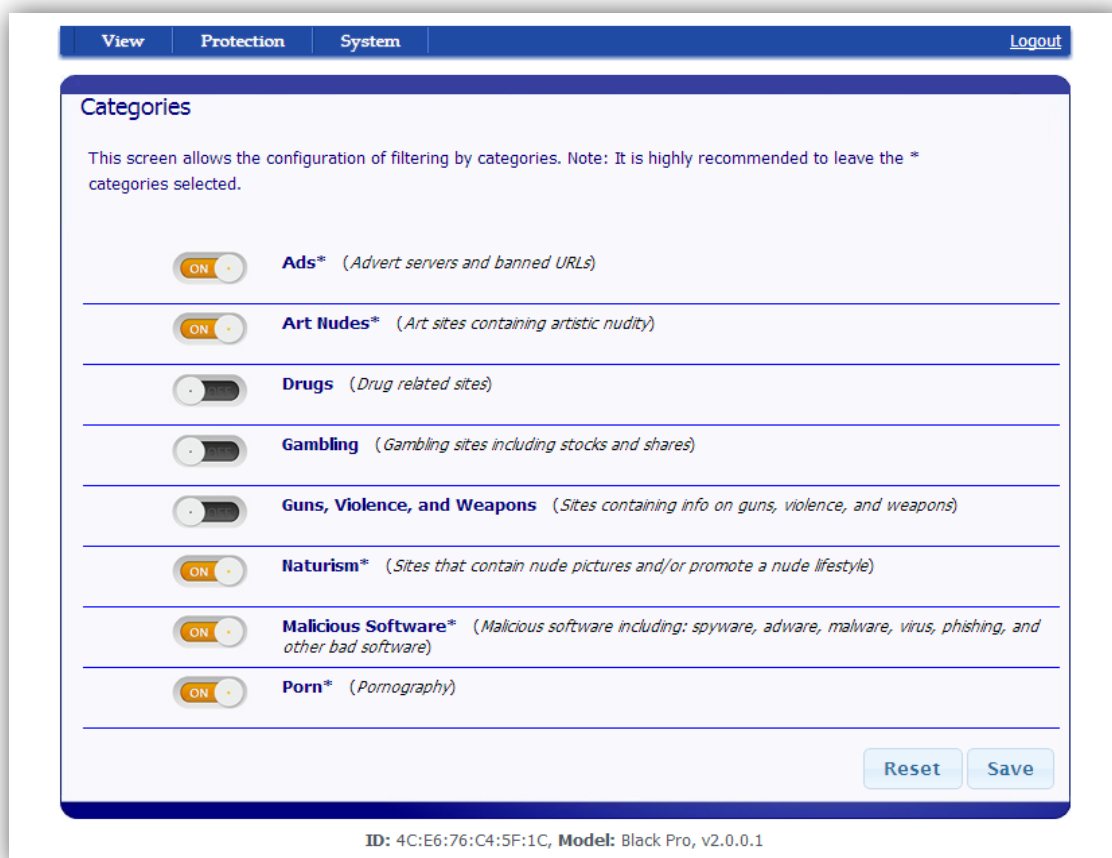
### 4.2g: Configuring the filter: Filtering Categories

Location: **Protection Tab > Categories**

The Categories page allows the user to easily customize the filtering mechanism, based on predefined categories.

To Activate/Deactivate a category :

- Press the corresponding switch.
- Click “Save” when all changes have been made





# Chapter 4:

## The Filtering Mechanism

### 4.2h: Configuring the filter: Exclude From Filter

**Location: Protection Tab > Exclude from Filter**

The Exclude from Filter tool allows the user to disable the filtering system entirely for a specific device. This tool is especially useful for the following devices (Which Pandora's Hope **cannot** filter):

-DVRs (TiVo, Dish Hopper)

-Media players (Roku , Apple TV)

**To use the Exclude from Filter tool:**

- Enter in the MAC address for the device into the "Add MAC address" field, or use the "This Computer" function (If the device is connected to Pandora's Hope, then the DHCP Clients page will also list the MAC address)
- Click "Add" once the MAC address has been entered
- Press "Save" once all of the desired MAC addresses have been entered
- To **remove** a device from the exclusion list, click on the red "X" next to the MAC address. Then click "Save"

The screenshot shows a web interface with a blue header bar containing tabs for 'View', 'Protection', and 'System', and a 'Logout' link on the right. The main content area is titled 'Exclude from Filter' and contains a descriptive paragraph: 'This is a list of computers or devices that should not be filtered. Typically this will only be devices used for VoIP or streaming video. Add a Mac address into a list. It should be in format xx:xx:xx:xx:xx:xx'. Below this is a section labeled 'Add MAC address' with a text input field, a 'This Computer' button, and an 'Add' button. At the bottom right of the main content area are 'Reset' and 'Save' buttons. The footer of the page displays the ID '4C:E6:76:C4:5F:1C' and the Model 'Black Pro, v2.0.0.1'.

# Chapter 4:

## The Filtering Mechanism

### 4.2i: Configuring the filter: Time Restrictions

**Location:** Protection Tab > Time Restrictions

The Time Restriction function allows the user to specify when a particular device is able to access the internet.

Each Time Restriction rule applies to a single device, and each device can only have a single rule. A Time Restriction rule will activate and deactivate precisely, based on the schedule set. If a user attempts to use the internet during a restricted time, a blocking page will be displayed, informing them of the restriction. This blocking page can be bypassed, using the administrative password. Once bypassed, the user will automatically be directed to the administrative interface, where they can disable the Time Restriction rule.

**More information on Time Restrictions can be found on the following page**



The screenshot shows a web interface with a blue header bar containing tabs for 'View', 'Protection', 'System', and a 'Logout' link. The 'Protection' tab is active. Below the header, the page title is 'Time Restrictions'. The main content area is light blue and contains the text: 'Add a MAC address of your device and determine an hours when it is allowed to access an internet. MAC address should be in format xx:xx:xx:xx:xx:xx'. There is a large empty text input field for the MAC address. To the right of the input field is a blue 'Add' button. At the bottom right of the main content area are two blue buttons: 'Reset' and 'Save'. At the very bottom of the page, below the main content area, is a footer line that reads: 'ID: 4C:E6:76:C4:5F:1C, Model: Black Pro, v2.0.0.1'.

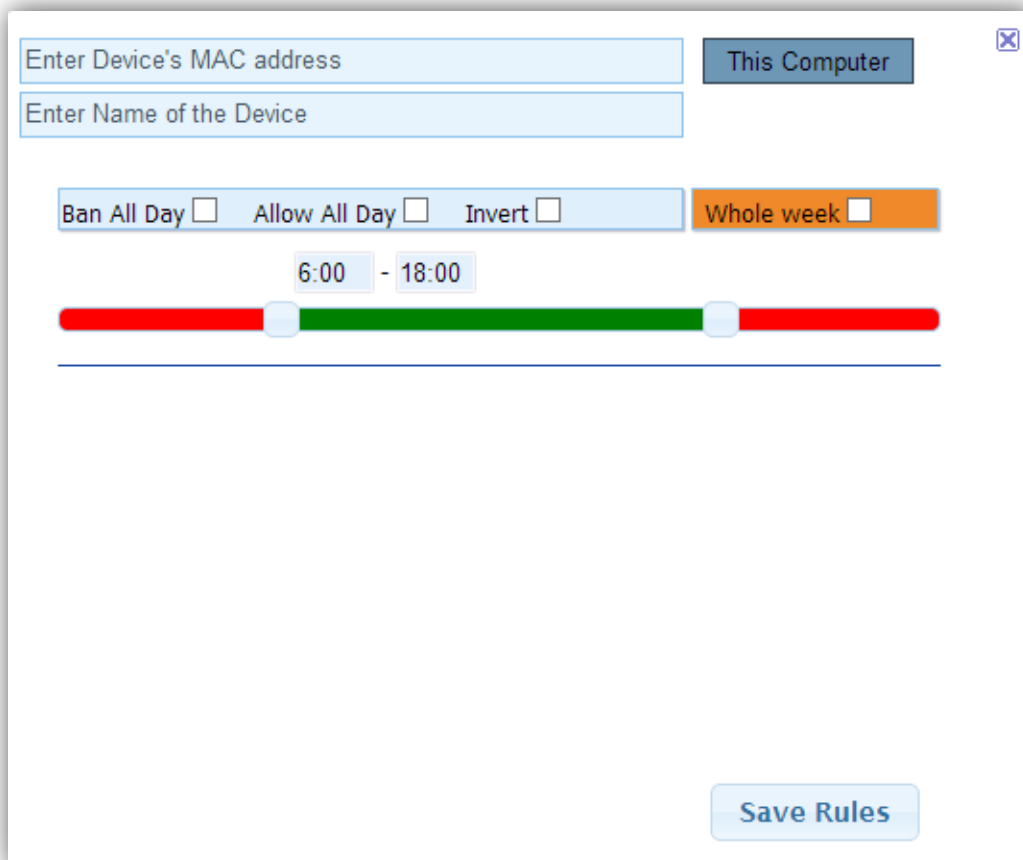
# Chapter 4:

## The Filtering Mechanism

### 4.2i: Configuring the filter: Time Restrictions (Continued)

To use the Time restriction function:

- Enter in the MAC address for the device into the “Device’s MAC” field, or use the “This Computer” function (If the device is connected to Pandora’s Hope, then the DHCP Clients page will also list the MAC address)
- Label the Time Restriction rule by entering a name into the “Enter Name” field
- There are four check boxes that define part of the rule:
  - Ban All Day will restrict the device for the entire day (or days)
  - Allow All Day will permit internet access for the entire day (or days)
  - Invert will reverse the “Allowed” and “Restricted” ranges.
  - Whole week allows each individual day to be customized with a different range.
- Once the desired values have been set, the “Save Rules” button must be pressed to activate the rule
- To edit an existing rule, press the “Pencil” icon next to the rule
- To remove a rule, press the red “X” next to the rule



The screenshot shows a configuration window for time restrictions. It features two input fields at the top: "Enter Device's MAC address" and "Enter Name of the Device". To the right of these fields is a button labeled "This Computer" and a close icon (X). Below the input fields, there are four checkboxes: "Ban All Day", "Allow All Day", "Invert", and "Whole week". The "Ban All Day" checkbox is currently checked. Below the checkboxes, there is a time range selector showing "6:00 - 18:00". This is represented by a horizontal bar with a red segment on the left, a green segment in the middle, and a red segment on the right. The green segment is currently selected. At the bottom right of the window is a button labeled "Save Rules".

# Chapter 4:

## The Filtering Mechanism

### 4.2j: Configuring the filter: Ad-Driven Websites

**Location: Protection Tab > Ad-Driven Sites**

The Ad-Driven Sites tool allows the user to disable the ad-blocking service on Pandora's Hope for a particular webpage. This is useful for viewing websites that require advertisements to function.

**To add an entry into the Ad-Driven sites tool:**

- Enter in the web address into the blue area .  
(**Note:** You do not need the prefixes HTTP: or WWW.)
- Click the "Add" button
- Once all of the desired addresses have been added, click "Save"
- The newly added websites will be permitted to display advertisements immediately after pressing "Save"

**To remove an entry from the Ad-Driven Sites tool:**

- Press the red "X" next to the web address
- Once all of the desired web addresses have been removed, click "Save"

#### Ad Driven Sites

TV Sites (such as NBC, CBS, ABC, etc.) often are ad driven. In order for you to be able to view episodes online, these sites need to allow ads. Entering the sites below will trigger the ad-blocking to be turned-off for 90 minutes so you can view your episodes. If a site is being blocked, you can add it to the list below.

X

abc.go.com

X

cbs.com

X

fox.com

X

nbc.com

X

cwtv.com

X

espn.go.com

# Chapter 4:

## The Filtering Mechanism

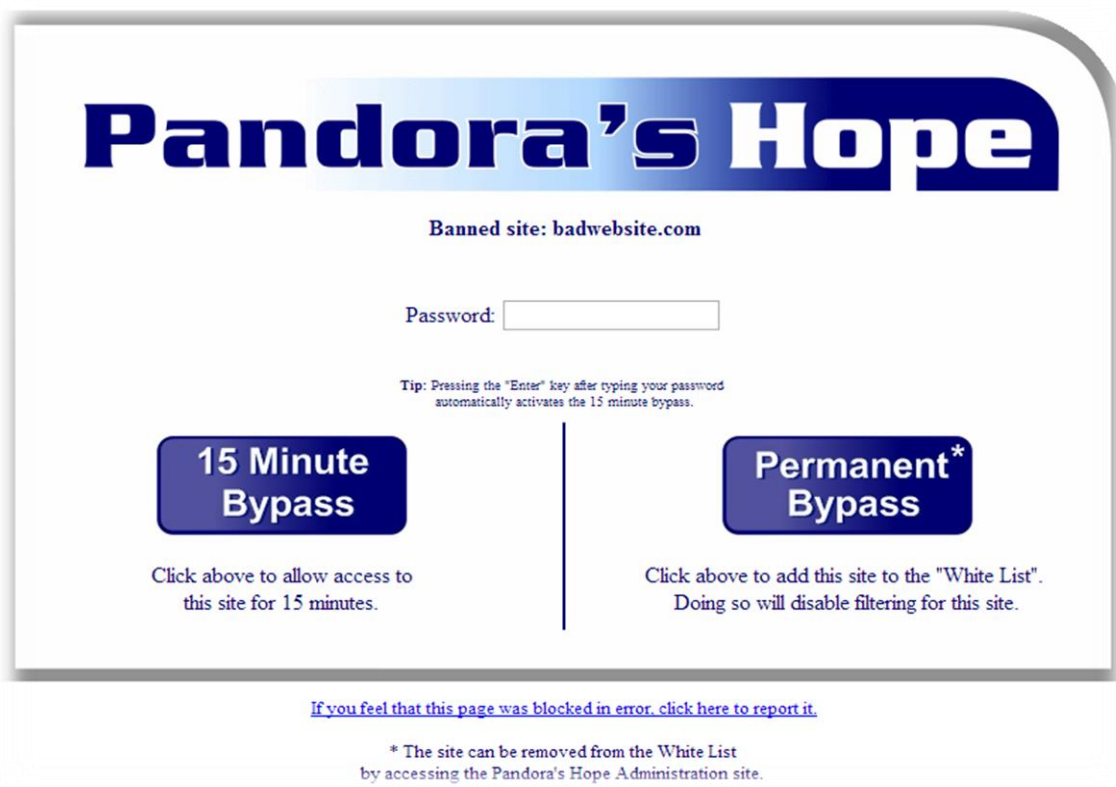
### 4.3: The Blocking Page

The “Blocking Page” is the webpage displayed when inappropriate content has been detected. This page allows the user to bypass a block, either temporarily (15 minutes), or permanently (The website is white listed).

To authorize a bypass:

- Enter the administrative password into the “Password” field
- Select the Temporary, or Permanent options.  
(The Temporary option is usually the safest)

**Important:** Using the Bypass option will leave the destination website **unfiltered**



The image shows a screenshot of a web page titled "Pandora's Hope" in a large, bold, blue font. Below the title, it says "Banned site: badwebsite.com". There is a "Password:" label followed by a text input field. Below the input field, a tip states: "Tip: Pressing the 'Enter' key after typing your password automatically activates the 15 minute bypass." There are two large blue buttons with white text: "15 Minute Bypass" and "Permanent\* Bypass". Below the "15 Minute Bypass" button, it says "Click above to allow access to this site for 15 minutes." Below the "Permanent\* Bypass" button, it says "Click above to add this site to the 'White List'. Doing so will disable filtering for this site." At the bottom, there is a link: "If you feel that this page was blocked in error, click here to report it." and a footnote: "\* The site can be removed from the White List by accessing the Pandora's Hope Administration site."

**Pandora's Hope**

Banned site: badwebsite.com

Password:

Tip: Pressing the "Enter" key after typing your password automatically activates the 15 minute bypass.

**15 Minute Bypass**

Click above to allow access to this site for 15 minutes.

**Permanent\* Bypass**

Click above to add this site to the "White List". Doing so will disable filtering for this site.

[If you feel that this page was blocked in error, click here to report it.](#)

\* The site can be removed from the White List by accessing the Pandora's Hope Administration site.

# Chapter 5:

## System Settings

### 5.1: Wireless Configuration

**Location:** System > Wireless Configuration

The Wireless Configuration page allows the user to change various aspects of the wireless network. Descriptions of the options found on this page are located below.

**Important! The settings on this page have the ability to bring down the wireless network. Use with caution.**

#### Option Descriptions:

-*Enable Wireless access:* This will Activate or Deactivate the wireless network

-*Channel:* This will change the wireless channel. By default this value is set to "5"

-*Broadcast SSID:* This will show or hide the wireless network name (SSID)

-*SSID:* This is the name of the wireless network

-*Enable Wireless Security:* This enables or disables wireless network security

-*Security Type:* Changes the wireless security standard. By default this is set to "WPA2"

-*Key:* This is the wireless network security key, used to connect wireless devices to Pandora's Hope

-*Enable MAC Filtering:* This enables the MAC filtering option, which can be used to prevent devices with specific MAC addresses from connecting to the wireless network.

-*Protocol:* This sets the IEEE wireless standard to be used. By default this is set to "11ng."

-*Channel Width:* This changes the width of the wireless channel. By default this is set to "40MHz Upper"

-*No Scan:* This option enables or disable the auto-scanning functionality of the router. By default it is set to "On"

**Pro version users:** There will be a second radio, which will also have the settings above. This is for the 5Ghz radio.

# Chapter 5:

## System Settings

### 5.1a: Wireless Configuration (Continued)

This is the wireless configuration page

ViewProtectionSystemLogout

Wireless Configuration

This screen is to specify your basic wireless settings. Manage Wireless status, SSID, security and filtering.

Radio 1

Wireless status & a channel

ON

Enable Wireless

5

Channel

Unique SSID name & Broadcast settings

ON

Broadcast SSID

PandorasHope

SSID

Wireless security

ON

Enable Wireless Security

WEP

Protection Type/Strength

3453453456

Wireless key

MAC Filtering

OFF

Enable MAC Filtering

Misc

11ng

Protocol

HT40+ (2x20MHz -/+)

Channel Width

ON

Noscan

# Chapter 5:

## System Settings

### 5.2a: Network Configuration: General Settings

**Location:** System > General

The General page contains settings that allow the user to change the IP addressing of the WAN, and LAN interfaces.

**Important! The settings on this page have the ability to render Pandora's Hope inoperable. Use with caution.**

#### Internet/WAN Settings

-The "Connect Via" drop-down menu allows the user to set the WAN interface to a static address. This is usually reserved for special circumstances, where an ISP's equipment requires the use of a static IP address. When switching to a static address, the user will need to populate the new settings with information provided from their ISP.

#### Local Network / LAN Settings

-The "Router IP" field allows the user to change the IP addressing scheme for Pandora's Hope. By default, Pandora's Hope uses the **192.168.2.1** network.

-The "Subnet Mask" field allows the user to set the appropriate subnet mask information.

The screenshot shows the 'General' settings page in the Pandora's Hope web interface. At the top, there are tabs for 'View', 'Protection', and 'System', with 'System' being the active tab. A 'Logout' link is in the top right corner. The main heading is 'General', followed by a warning: 'This screen contains advanced settings that could cause you to be unable to connect to your router. Please only configure this page if you are certain you know what their changes will cause.' Below this, there are two sections: 'Internet / WAN' and 'Local Network / LAN'. The 'Internet / WAN' section shows 'Current IP: 192.168.2.1', a 'DHCP' dropdown menu, and a 'Connect Via' button. The 'Local Network / LAN' section shows 'Router IP:' with a text field containing '192.168.2.1' and 'Subnet Mask:' with a text field containing '255.255.255.0'. At the bottom right, there are 'Reset' and 'Save' buttons. At the very bottom, the device ID 'ID: 4C:E6:76:C4:5F:1C' and model 'Model: Black Pro, v2.0.0.1' are displayed.

View Protection System Logout

### General

This screen contains advanced settings that could cause you to be unable to connect to your router. Please only configure this page if you are certain you know what their changes will cause.

Internet / WAN

Current IP: 192.168.2.1 DHCP Connect Via

Local Network / LAN

Router IP: 192.168.2.1 Subnet Mask: 255.255.255.0

Reset Save

ID: 4C:E6:76:C4:5F:1C, Model: Black Pro, v2.0.0.1



# Chapter 5:

## System Settings

### 5.2b: Network Configuration: Port Forwarding

**Location:** System > Port Forwarding

The Port Forwarding tool allows the user to permit and redirect incoming information through specific ports, for a particular device. This tool is useful in getting some applications and devices working through Pandora's Hope, which may require a specific port to be open.

**To create a port forwarding rule:**

- Enter in a name for the new rule in the "Application Name" field.
- Enter in the "From port" number. This will be the original port number
- Enter in the IP address for the device you would like the rule to govern.
- Enter in the "To port" number. This number is set by the user.
  - If the "To" and "From" ports are identical, traffic across that port will not be redirected, but permitted
  - If the "To" and "From" ports differ, traffic coming through the "From" port will be redirected to the "To" port
- Select the Protocol to be used by the port forwarding rule.
- To create the new port forwarding rule, press the "Add" button
- Once all of the desired rules have been added, press "Save"

The screenshot shows a web-based configuration interface for Port Forwarding. At the top, there is a navigation bar with tabs for 'View', 'Protection', and 'System', and a 'Logout' link on the right. The main heading is 'Port Forwarding', followed by a sub-heading 'Forward Individual Ports From Internet/WAN to local services/LAN.' Below this, there are four input fields: 'Application Name' (a text box), 'From Port\*' (a text box), 'IP Address\*' (a text box), and 'To Port\*' (a text box). To the right of the 'Application Name' field is a 'Protocol\*' dropdown menu currently set to 'Both'. An 'Add' button is positioned below the 'To Port\*' field. At the bottom right, there are 'Reset' and 'Save' buttons. The footer of the interface displays the ID '10:6F:3F:02:A5:49' and the Model 'v2.0.0.1'.

# Chapter 5:

## System Settings

### 5.2c: Network Configuration: DHCP Settings

**Location:** System > DHCP Settings

The DHCP Settings page allows the user to create static leases for their devices. A static lease prevents the IP address of a computer from changing.

**To create a static lease:**

- Enter in a name in the “Name” field. This name is superficial, and can be whatever the user prefers.
- Enter in the desired IP address for the device in the “IP” field
- Enter in the MAC address for the device in the “MAC” field (See page [3.4](#) for more information)
- Once all of the required information has been entered, press Add.
- Once all of the desired static leases have been entered, press Save

The screenshot shows a web interface for DHCP settings. At the top, there is a navigation bar with tabs for 'View', 'Protection', 'System', and a 'Logout' link. The main content area is titled 'DHCP' and includes the instruction 'Configure your Dynamic Host Control Protocol.' Below this, there are three main sections: 'Active leases' (currently empty), 'Add Static lease', and 'Static leases' (also empty). The 'Add Static lease' section contains three input fields: 'Name', 'IP', and 'MAC'. An 'Add' button is positioned to the right of the 'MAC' field. At the bottom right of the main content area, there are 'Reset' and 'Save' buttons. A footer at the very bottom of the page displays the device ID '4C:E6:76:C4:5F:1C' and the model 'Black Pro, v2.0.0.1'.

# Chapter 5:

## System Settings

### 5.2d: Network Configuration: UPnP

**Location:** System > UPnP

The Universal Plug-n-Play tool allows the user to modify UPnP settings. UPnP is a set of network protocols, that allows networked devices to automatically discover each other. These settings should remain unchanged, unless the user has a specific reason to modify them.

The screenshot shows a web interface for configuring UPnP settings. At the top, there is a navigation bar with tabs for 'View', 'Protection', and 'System', and a 'Logout' link on the right. The main content area is titled 'UPnP' and contains a description: 'Tool to configure Universal Plug-n-Play Internet Gateway service. Enable or disable the service and set limits to access UPnP from internet.' Below this, there are three configuration options: 'UPNP Daemon' set to 'Enabled' (with a dropdown arrow), 'WAN Upload (bits/sec)' set to '512' kbps, and 'WAN Download (bits/sec)' set to '1024' kbps. At the bottom right, there are 'Reset' and 'Save' buttons. The footer of the page displays the device ID '4C:E6:76:C4:5F:1C' and the model 'Black Pro, v2.0.0.0'.

UPnP		
Tool to configure Universal Plug-n-Play Internet Gateway service. Enable or disable the service and set limits to access UPnP from internet.		
<b>UPNP Daemon</b>	Enabled	
<b>WAN Upload (bits/sec)</b>	512	kbps
<b>WAN Download (bits/sec)</b>	1024	kbps
<a href="#">Reset</a> <a href="#">Save</a>		

ID: 4C:E6:76:C4:5F:1C, Model: Black Pro, v2.0.0.0

# Chapter 5:

## System Settings

### 5.3: User Information

**Location:** System > User Information

The User Information page displays the personal information of the account holder. This information can be modified at any time through this page.

**To update the user's information:**

- Make the necessary changes.
- When all changes have been made, press Save

The screenshot shows a web interface with a blue header bar containing tabs for 'View', 'Protection', and 'System', and a 'Logout' link on the right. The main content area is titled 'User Information' and contains a descriptive text: 'View and update the email addresses your router uses to communicate with you. Enter your name and phone number.' Below this text are four input fields with labels: 'Name\*' (containing 'Mr. Pandora's Hope'), 'Email\*' (containing 'Support@PandorasHope.com'), 'Secondary Email' (containing 'Optional@NotManditory.com'), and 'Phone' (containing '520-445-4673'). At the bottom right of the form are 'Reset' and 'Save' buttons. The footer of the page displays the text 'ID: 10:6F:3F:02:A5:49, Model: , v2.0.0.1'.

Field	Value
Name*	Mr. Pandora's Hope
Email*	Support@PandorasHope.com
Secondary Email	Optional@NotManditory.com
Phone	520-445-4673

# Chapter 5:

## System Settings

### 5.4: Resetting the Administrative Password

**Location:** System > Password

The Password tool allows the user to change the administrative password.

**To create a new password:**

- Enter in the desired password in the “Password” field.
- Confirm this password in the “Confirm Password” field.
- Once the new password has been entered in twice, press Save

**Important! If the administrative password has been lost, the user will need to contact the Pandora’s Hope support team:**

**1-520-445-4673**

**Support@PandorasHope.com**

The screenshot shows a web interface for changing the administrative password. At the top, there is a navigation bar with tabs for 'View', 'Protection', 'System', and a 'Logout' link. The 'System' tab is selected. Below the navigation bar, the page title is 'Password'. The main content area has the instruction 'Change your password below.' followed by two input fields: 'Password' and 'Confirm Password'. At the bottom right of the form, there are two buttons: 'Reset' and 'Save'. At the very bottom of the page, there is a footer with the text 'ID: 4C:E6:76:C4:5F:1C, Model: Black Pro, v2.0.0.0'.

